

Guia para criar senhas fortes

Segurança da Informação



Informativos Gerais



Guia para criar senhas fortes

Introdução

A Rede Américas está comprometida com segurança das informações e proteção de dados, sejam eles corporativos ou pessoais. Uma senha forte é a primeira e, uma das mais importantes, etapas de defesa contra ameaças digitais.

O uso de senhas fracas e repetidas aumenta consideravelmente os riscos de ataques cibernéticos, como roubo de identidade, acessos não autorizados a contas e vazamento de informações sensíveis.

Pensando nisso, elaboramos um guia prático para você criar senhas seguras e fortes.

Por que senhas fortes são importantes?

Senhas são como chaves que protegem informações valiosas. Uma senha fraca pode ser facilmente descoberta por criminosos digitais, colocando em risco seus dados pessoais, financeiros, dados de pacientes e até informações confidenciais da Rede Américas.

Como criar uma senha forte?

1 Use no mínimo 12 caracteres: quanto mais longa a senha, mais difícil será descobri-la.

2 Combine diferentes tipos de caracteres:

- Letras maiúsculas (A, B, C...);
- Letras minúsculas (a, b, c...);
- Números (1, 2, 3...);
- Símbolos especiais (@, #, %, &...).

Exemplo: S3gur@ncA2025!

3 Evite informações pessoais: não use dados fáceis de adivinhar, como nomes, datas de aniversário ou o nome do seu animal de estimação.

4 Evite padrões previsíveis: senhas como "123456", "senha123" ou "abcdef".

5 Pense numa frase fácil de lembrar e transforme-a em uma senha forte.

Frase "Eu tomo café com leite sem açúcar todo dia às 8h da manhã!"

- Utilize a primeira letra de cada palavra e o símbolo especial usado na frase;
- Para tornar a senha ainda mais forte, você pode substituir alguma letra por um número ou símbolo especial. Neste exemplo, substituímos a primeira letra "a" da palavra "açúcar" por "@".

Senha: Etccls@tda8dm!

Dicas para gerenciar suas senhas

- **Não reutilize senhas:** use senhas diferentes para cada conta ou sistema. Isso garante que, mesmo que uma senha seja comprometida, as outras continuem seguras;
- **Atualize senhas periodicamente:** altere suas senhas a cada 6 (seis) meses ou sempre que houver suspeita de comprometimento;
- **Ative múltiplo fator de autenticação (MFA):** sempre que possível, habilite o MFA. Essa camada extra de segurança solicita uma confirmação adicional, como um código enviado ao seu celular. Você pode utilizar aplicativos como, por exemplo, o Microsoft Authenticator;
- **Não anote senhas em lugares inseguros:** não escreva senhas em papéis ou em arquivos não protegidos no seu computador ou celular;
- **Teste sua senha:** use ferramentas seguras para verificar a força da sua senha (evite testar senhas reais em sites não confiáveis).
Ex: [Kaspersky Password Checker](#)
- **Cuidado com golpes:** não compartilhe suas senhas por e-mail, mensagens ou telefonemas. Nenhuma empresa séria solicita senhas dessa forma.

Conclusão

Uma boa senha é um pequeno esforço que pode proteger você, nossos pacientes e a Rede Américas contra desafios indesejados. Fique em segurança e compartilhe este guia com seus colegas.

A segurança da informação, proteção dos dados e continuidade do negócio começa com você.

Pequenos cuidados no dia a dia fazem a diferença.



Rede Américas

paixão por cuidar